



THE UNIVERSITY *of* EDINBURGH

Edinburgh Research Explorer

## OGC® Engineering Report for the OWS Shibboleth Interoperability Experiment

### Citation for published version:

Higgins, C 2012, *OGC® Engineering Report for the OWS Shibboleth Interoperability Experiment*. OGC Public Engineering Reports, Open Geospatial Consortium. <<http://www.opengeospatial.org/standards/per>>

### Link:

[Link to publication record in Edinburgh Research Explorer](#)

### Document Version:

Early version, also known as pre-print

### General rights

Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

### Take down policy

The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact [openaccess@ed.ac.uk](mailto:openaccess@ed.ac.uk) providing details, and we will remove access to the work immediately and investigate your claim.



# Open Geospatial Consortium

Approval Date: 2012-03-23

Publication Date: 2012-04-06

**External identifier of this OGC® document:** <http://www.opengis.net/doc/ER/ows-shibboleth-ie>

Reference number of this document: OGC 11-019r2

Category: Public Engineering Report

Editor: Chris Higgins

## **OGC® Engineering Report for the OWS Shibboleth Interoperability Experiment**

Copyright © 2012 Open Geospatial Consortium

To obtain additional rights of use, visit <http://www.opengeospatial.org/legal/>.

### **Warning**

This document is not an OGC Standard. This document is an OGC Public Engineering Report created as output from an Interoperability Experiment – an Interoperability Program initiative – and does not represent an official position of the OGC. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an OGC Standard. Further, any OGC Engineering Report should not be referenced as required or mandatory technology in procurements.

Document type:	OpenGIS® Engineering Report
Document subtype:	NA
Document stage:	Approved for public release
Document language:	English

## **Abstract**

This document reports on outcomes from the OGC Web Services Shibboleth Interoperability Experiment (OSI). The main objective of OSI was to advance the use of Shibboleth (an open source implementation of SAML) as a means of protecting OWS. In the process, OSI helped develop further understanding of this approach to establishing trusted federations of OWS. This report documents these findings and is intended to be of use to those interested in how Shibboleth/SAML access management federations may function as an organisational model for operational Spatial Data Infrastructure.

## License Agreement

Permission is hereby granted by the Open Geospatial Consortium, ("Licensor"), free of charge and subject to the terms set forth below, to any person obtaining a copy of this Intellectual Property and any associated documentation, to deal in the Intellectual Property without restriction (except as set forth below), including without limitation the rights to implement, use, copy, modify, merge, publish, distribute, and/or sublicense copies of the Intellectual Property, and to permit persons to whom the Intellectual Property is furnished to do so, provided that all copyright notices on the intellectual property are retained intact and that each person to whom the Intellectual Property is furnished agrees to the terms of this Agreement.

If you modify the Intellectual Property, all copies of the modified Intellectual Property must include, in addition to the above copyright notice, a notice that the Intellectual Property includes modifications that have not been approved or adopted by LICENSOR.

THIS LICENSE IS A COPYRIGHT LICENSE ONLY, AND DOES NOT CONVEY ANY RIGHTS UNDER ANY PATENTS THAT MAY BE IN FORCE ANYWHERE IN THE WORLD.

THE INTELLECTUAL PROPERTY IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE INTELLECTUAL PROPERTY WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE INTELLECTUAL PROPERTY WILL BE UNINTERRUPTED OR ERROR FREE. ANY USE OF THE INTELLECTUAL PROPERTY SHALL BE MADE ENTIRELY AT THE USER'S OWN RISK. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR ANY CONTRIBUTOR OF INTELLECTUAL PROPERTY RIGHTS TO THE INTELLECTUAL PROPERTY BE LIABLE FOR ANY CLAIM, OR ANY DIRECT, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM ANY ALLEGED INFRINGEMENT OR ANY LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR UNDER ANY OTHER LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH THE IMPLEMENTATION, USE, COMMERCIALIZATION OR PERFORMANCE OF THIS INTELLECTUAL PROPERTY.

This license is effective until terminated. You may terminate it at any time by destroying the Intellectual Property together with all copies in any form. The license will also terminate if you fail to comply with any term or condition of this Agreement. Except as provided in the following sentence, no such termination of this license shall require the termination of any third party end-user sublicense to the Intellectual Property which is in force as of the date of notice of such termination. In addition, should the Intellectual Property, or the operation of the Intellectual Property, infringe, or in LICENSOR's sole opinion be likely to infringe, any patent, copyright, trademark or other right of a third party, you agree that LICENSOR, in its sole discretion, may terminate this license without any compensation or liability to you, your licensees or any other party. You agree upon termination of any kind to destroy or cause to be destroyed the Intellectual Property together with all copies in any form, whether held by you or by any third party.

Except as contained in this notice, the name of LICENSOR or of any other holder of a copyright in all or part of the Intellectual Property shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Intellectual Property without prior written authorization of LICENSOR or such copyright holder. LICENSOR is and shall at all times be the sole entity that may authorize you or any third party to use certification marks, trademarks or other special designations to indicate compliance with any LICENSOR standards or specifications.

This Agreement is governed by the laws of the Commonwealth of Massachusetts. The application to this Agreement of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded. In the event any provision of this Agreement shall be deemed unenforceable, void or invalid, such provision shall be modified so as to make it valid and enforceable, and as so modified the entire Agreement shall remain in full force and effect. No decision, action or inaction by LICENSOR shall be construed to be a waiver of any rights or remedies available to it.

None of the Intellectual Property or underlying information or technology may be downloaded or otherwise exported or reexported in violation of U.S. export laws and regulations. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use the Intellectual Property, and you represent that you have complied with any regulations or registration procedures required by applicable law to make this license enforceable.

<b>Contents</b>	<b>Page</b>
1 Introduction.....	1
1.1 Scope of document .....	1
1.2 Document contributor contact points .....	1
1.3 Revision history.....	1
1.4 Future work .....	1
1.5 Forward .....	2
2 References.....	2
3 Terms and definitions .....	3
4 Conventions .....	3
4.1 Abbreviated terms .....	3
5 OGC Web Services Shibboleth IE Overview .....	3
5.1 Security Assertion Markup Language (SAML) .....	4
5.2 Shibboleth.....	6
5.3 The ESDIN Project.....	8
5.3.1 The ESDIN Federation .....	8
5.4 Scope of the IE .....	8
5.4.1 Within scope .....	9
5.4.2 Out of scope .....	9
6 Methodology .....	10
6.1 Component development.....	10
6.2 Technology Integration Experiment.....	10
7 Results.....	13
7.1 EDINA.....	14
7.2 Envitia .....	14
7.2.1 Envitia Experimentation with SAML/ECP Profile.....	15
7.2.2 Engagement in the Shibboleth IE .....	16
7.2.3 Envitia Conclusions .....	18
7.3 Joint Research Centre (JRC) - Implementation of Shibboleth-based protected OGC Web Map Services and their access from the INSPIRE GeoPortal.....	19
7.3.1 Use Cases .....	19
7.3.2 Testing architecture.....	21
7.3.3 Experienced issues .....	23
7.3.4 Results and future work .....	24
8 Conclusions.....	24





## 1 Introduction

### 1.1 Scope of document

This document reports on outcomes from the OGC Web Services Shibboleth Interoperability Experiment (OSI). The main objective of OSI was to advance the use of Shibboleth (an open source implementation of SAML) as a means of protecting OWS. In the process, OSI helped develop further understanding of this approach to establishing trusted federations of OWS. This report documents these findings and is intended to be of use to those interested in how Shibboleth/SAML access management federations may function as an organisational model for operational Spatial Data Infrastructure.

### 1.2 Document contributor contact points

All questions regarding this document should be directed to the editor or the contributors:

Name	Organization	e-mail
Chris Higgins	EDINA	<a href="mailto:chris.higgins@ed.ac.uk">chris.higgins@ed.ac.uk</a>
Andreas Matheus	Secure Dimensions GmbH	Am(at)secure-dimensions.com

### 1.3 Revision history

Date	Release	Editor	Primary clauses modified	Description
Feb 2011	V1.0.0	Chris Higgins	Initial ER	First draft in time for the Bonn TC
Feb 2011	V1.0.1	Andreas Matheus	Throughout	Comments, edits and corrections
Feb 2012	V2.0.0	Chris Higgins	Second draft. Results section	Mainly additions to the results sections from those IE participants who provided text.

### 1.4 Future work

The work described in this document describes a solution to a fundamental problem obstructing the advancement of Spatial Data Infrastructures (SDI) - where resources need to be protected, how can OWS in different administrative domains be secured in a genuinely interoperable way so that only properly authenticated users gain access? This



has the potential to lead to a significant amount of future work in many different related areas; some of which is documented here and in related publications, eg, Higgins et al, 2012.

In particular, this document would be improved by greater detail being made available by implementing organizations on the issues encountered when modifying client software to undergo Shibboleth/SAML interactions and broader issues encountered when employing SAML access management federations to secure SDI.

While Shibboleth presents a valuable open source and ad hoc SAML reference implementation, it should be noted that SAML components are already widely in use throughout the GI industry. It may be anticipated that future work will involve the use of both open source and commercial implementations.

## 1.5 Forward

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The Open Geospatial Consortium Inc. shall not be held responsible for identifying any or all such patent rights.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the standard set forth in this document, and to provide supporting documentation.

## 2 References

The following documents are referenced in this document. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. For undated references, the latest edition of the normative document referred to applies.

Higgins, C., Koutroumpas, M., Matheus, A. and Seales, A (2012). “Shibboleth Access Management Federations as an Organisational Model for SDI”. International Journal of Spatial Data Infrastructures Research, Vol 7 (2012).

<http://ijdsdir.jrc.ec.europa.eu/index.php/ijdsdir/article/viewFile/245/295> [accessed Feb 2012]

OGC 06-121r3, *OpenGIS® Web Services Common Standard*

OGC 06-042, *OpenGIS® Web Map Service Implementation Specification, Version 1.3.0*

OGC 04-094, *OpenGIS® Web Feature Service (WFS) Implementation Specification, Version 1.1.0*

OASIS 2005, *Security Assertion Markup Language (SAML), Version 2.0*

OASIS 2005, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0

OASIS 2005, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0

### **3 Terms and definitions**

For the purposes of this report, the definitions specified in Clause 4 of the OWS Common Implementation Specification [OGC 06-121r3] shall apply. In addition, the definitions in OASIS SAML 2.0 shall apply.

### **4 Conventions**

#### **4.1 Abbreviated terms**

SAML      Security Assertion Markup Language

IdP        Identity Provider

SP        Service Provider

SSO       Single Sign On

SDI        Spatial Data Infrastructure

### **5 OGC Web Services Shibboleth IE Overview**

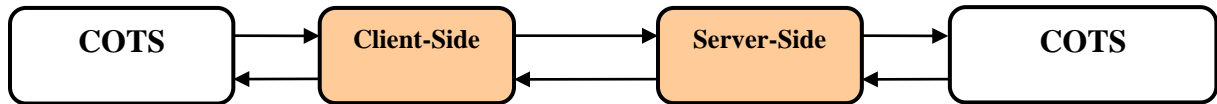
As described in the OGC Reference Model, OGC services are defined using open non-proprietary Internet standards such as HTTP, URL, MIME, XML, WSDL or SOAP. The usual interaction between clients and services is request-response, where the client first makes a request which is transferred by either HTTP GET or POST with XML/SOAP to the service and then expects a response back.

There are plenty of scenarios where the service needs to know the identity of the requesting party before processing the request. Such scenarios include typical authorization use-cases (different permissions are associated with different requesters) and auditing.

However, the OGC service specifications do not address the issue of transferring identity information together with the request. There have been plenty of approaches in the past addressing this issue both within the OGC, eg, through the activities of the GeoDRM DWG, GeoRM SWG, Security DWG, the OWS-3, OWS-4, OWS-5, OWS-6 initiatives, the Authentication IE, as well as through different non-OGC projects.

Although this issue has been a “hot topic” for more than 5 years, there is still no best practice of how to transfer identity information between OGC clients and services. The

consequence of this is that few COTS products natively support basic security functions such as authentication and access control and whenever security is involved, typically an architecture with proxies / facades gets deployed (see picture below).



There are various ways in which identity information can be transferred from the OGC client to the OGC service by leveraging the underlying transport protocols. Both HTTP and SOAP offer native support for embedding security information and there are several main-stream authentication protocols that leverage these features.

Most importantly, by embedding the identity information in the transfer protocol the OGC service specifications are not touched at all, so the existing level of interoperability is not altered in any way.

This IE set out to demonstrate publicly how this could be achieved with a range of clients using the Security Assertion Markup Language (SAML) standards from OASIS in association with the widely used open source implementation Shibboleth.

### 5.1 Security Assertion Markup Language (SAML)

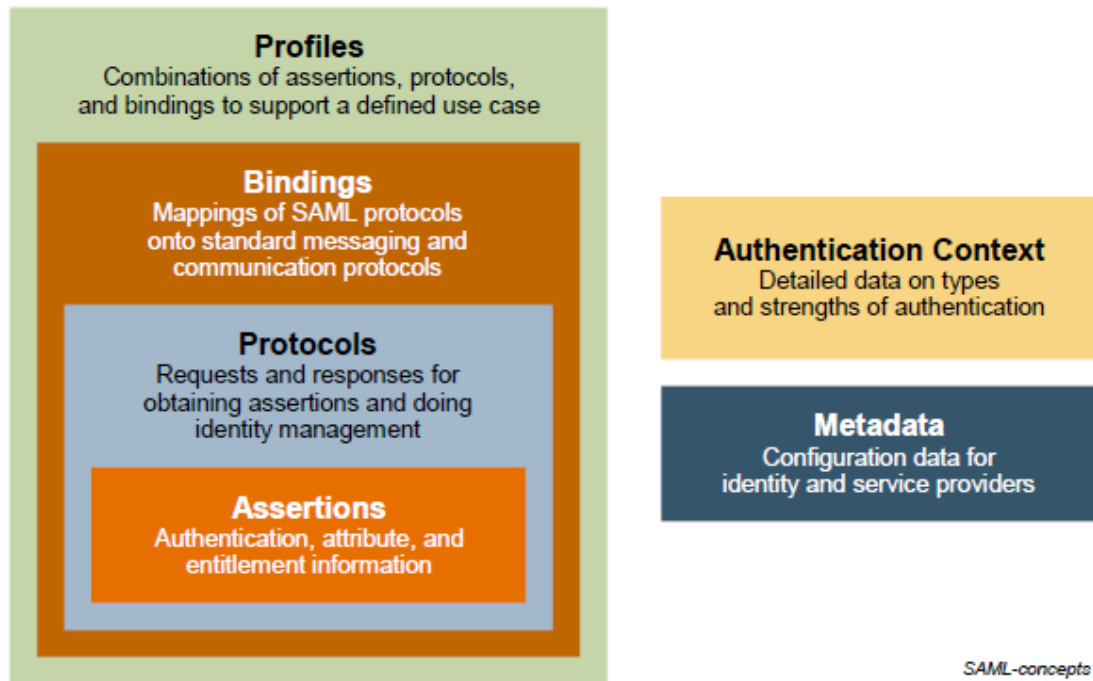
SAML is a product of the OASIS Security Services Technical Committee, it is an XML based open standard whose primary purpose is to enable the exchange of authentication data across security and policy domains.

The main use case for SAML is Single Sign On (SSO): with SSO users authenticate at one web site, access the resource of interest, and are then able to access additional protected resources at other web sites. SAML enables the communication of authentication information from the first site to additional sites in different security domains, these sites can then choose to authorise the user and allow access to the protected resource.

An organisational pre-requisite for the use of SAML in this scenario is the existence of an identity management federation. Federation in this case, means that a group of organisations with common business goals has established a circle of trust and formal understanding so that these cross-domain business interactions can take place.

Most organisations with valuable online resources will have some form of identity management in place, the decoupling and abstraction of identity management in federations required to make these cross security domain decisions is standardised in SAML. A key aspect is formal agreement on what security and identity information concerning the agent who is accessing the protected resource is required to enable

decisions to be taken as to whether they are authorised to access the resource or not. This information is communicated as assertions (see Fig 1 below)



**Fig 1 Basic SAML Concepts (from the SAML Technical Overview)**

Figure 1 has been included mainly to indicate some of the flexibility of SAML and to provide some background for the technical decisions made when implementing OWS clients. It has always been the intention that using Shibboleth to protect OWS should enable a wide range of different clients as typically found in SDI. The SAML2 components below support a number of use cases:

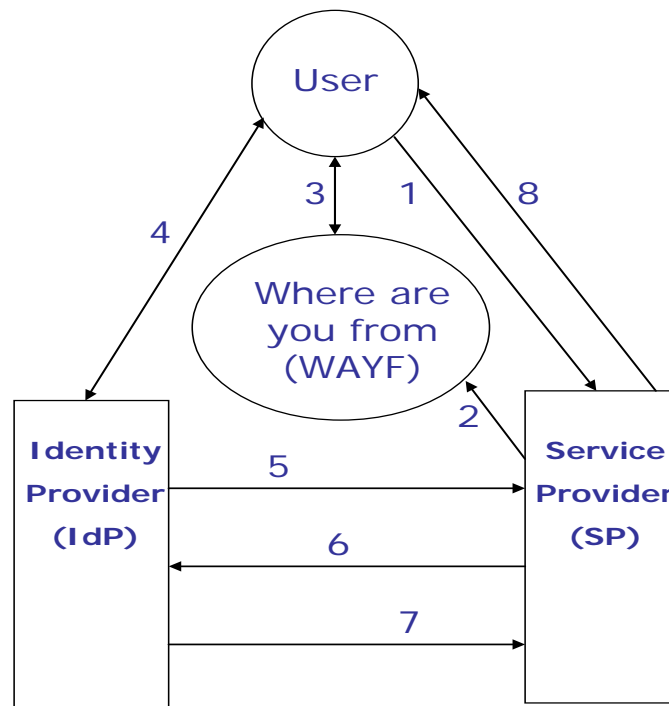
- **Assertions** are basic packets of information containing statements about a principal (that which wants to access the protected resource) that an asserting party, ie, an IdP, claims to be true. The SP then uses this information to make access control decisions. This attribute based model gives great flexibility, eg, under circumstances where the principals full identity is not important, cant be shared for privacy reasons or is insufficient for an authorisation decision without additional information.
- **Protocols** describe how assertions are packaged within SAML request and response elements, and gives the processing rules that SAML entities must follow when producing or consuming these elements.
- **Bindings** are mappings of SAML protocol message onto standard messaging formats and/or communications protocols, eg, SOAP, HTTP.

- **Profiles** describes in detail how SAML assertions, protocols, and bindings combine to support a defined use case. Two profiles were used in OSI to create two basic types of clients: Web Browser SSO Profile and Enhanced Client or Proxy (ECP) Profile.

## 5.2 Shibboleth

Shibboleth is an initiative from the US based Internet2 research and education networking consortium. It is an open source package that allows the establishment of federations of trusted Identity Providers and Service Providers based on SAML. It is a production strength solution to the problem of how to securely exchange user information based on open standards. Shibboleth is being used daily by 100s of millions of users around the globe and there are Shibboleth based access management federations in most developed countries, including most of Europe. For example, the UK Access Management Federation has approximately 8 million users.

Shibboleth is based on open security standards such as SAML (Security Access Markup Language), XML Signature, XML Encryption, etc. A decentralised approach is taken; organisations within the federation take responsibility for authenticating their own users using whichever method their organisation traditionally uses or prefers. In the language of Shibboleth, they act as Identity Providers (IdPs). Figure 2 provides an example series of Shibboleth exchanges typical of the UK Access Management Federation.



**Fig 2. Example Shibboleth Interactions**

1. User attempts to access a Shibboleth-protected resource on the Service Provider (SP) site.
2. User is redirected to the “Where are you from” (WAYF) in order to select their home organisation – typically synonymous with Identity Provider (IdP).
3. Part of same exchange as 2.
4. IdP ensures that user is authenticated, by whatever means IdP deems appropriate
5. After successful authentication, a one-time handle (a SAML artefact) is generated for this user session.
6. SP uses the handle to request attribute information from the IdP for this user
7. IdP allows or denies attribute information to be made available to this SP
8. Based on the attribute information made available, SP makes authorisation decision, ie, allows or denies the user access to the resource.

This may look complicated, but from the users perspective; they attempt to access a Shibboleth protected resource and the following happens:

- they gain access immediately as they have previously authenticated - Shibboleth supports SSO, or
- they get redirected to a list of organisations participating in the federation (WAYF) where,
- they select their home organisation and provide their (familiar) credentials for login to the home organisation
- they then either get access, or they don’t, with appropriate information supplied, eg, your institution does not subscribe to our service

Behind the scenes, there is what can be a complicated sequence of exchanges taking place, involving the resolution of SAML artefacts and the release of SAML assertions concerning the subject in accordance with the IdPs attribute release policy. Depending upon which SAML Profile or Binding is being used, this may be conducted over a secure encrypted back channel using SSL, SOAP, XML Encryption and XML Digital Signature.

Note that whereas the philosophy behind Shibboleth is to devolve responsibility as much as possible – in the belief that enterprises themselves are best positioned to manage the identities of their members, there are still some components that must be centralised. For example, in the UK Access Management Federation, the main WAYF (effectively a list mapping institution names to IdP URLs) is centralised in a trusted organisation, although many SPs choose to setup a decentralized WAYF (although there is still a dependency on the central WAFY). Of course, policy has to be centralized as well.

As might be expected in an area as delicate as sharing information about users, policy is often the most involved aspect in establishing access management federations. For example, each IdP maintains an attribute release policy. Which attributes get released depends upon who the agent is and the resource being protected. For example, in the UK, Data Protection Act considerations may prevent the users real name being made known (not necessarily a unique ID though), and certain attributes may only be released if its a student and SP 1, a lecturer and SP 2, etc.

### **5.3 The ESDIN Project**

The EU/eContentPlus funded European Spatial Data Infrastructure with a Best Practice Network (ESDIN) project started in 2008 and ended in 2011. The project consortium is comprised mainly of European National Mapping and Cadastral Agencies (NMCAs) and is led by EuroGeographics - a membership association that represents the interests of the NMCAs at the European level. A key goal for ESDIN is to assist European member states with preparation of their data for INSPIRE, including issues relating to security and access management.

#### **5.3.1 The ESDIN Federation**

The ESDIN Federation was a test Shibboleth Access Management Federation established during the lifetime of the project. It comprised of a number of NMCAs and European Universities - the latter as a secondary objective of ESDIN is to improve European academic sector access to NMCA data, partly using the offices of the OGC/AGILE/EuroSDR Persistent European Geospatial Testbed for Research and Education (PTB).

One important result of work undertaken in setting up the ESDIN Federation was the demonstration that OGC Web Services (OWS) can be protected using the mainstream Shibboleth download. No changes are required to either Shibboleth or the OGC interfaces in order to secure the OWS.

However, changes are required to the client applications. Building on an earlier project, the JISC funded SEE-GEO<sup>1</sup> project, a number of clients were developed during the course of ESDIN on top of open source software capable of undergoing the Shibboleth/SAML interactions.

### **5.4 Scope of the IE**

The main objective of the IE was to advance the use of Shibboleth in conjunction with OWS services. In doing so, we were aiming to develop implementation experience and flush out operational issues associated with this means of establishing trusted federations of OWS.

---

<sup>1</sup> <http://edina.ac.uk/projects/seesaw/seegeo/>

#### 5.4.1 Within scope

- Development of a number of OWS client applications capable of transferring identity information using Shibboleth
- Expansion of the ESDIN Federation to provide the best possible basis for demonstration purposes
- Demonstration of a variety of different vendor clients accessing Shibboleth protected OWS.
- Provision of findings as an engineering report (this document) that **may** be taken forward as a candidate Best Practices document.
- Provision of findings as part of an ESDIN Best Practice paper for use by organisations:
  - seeking to create Shibboleth Access Management Federations where a significant number of the service providers are providing OWS
  - wanting to setup services within Shibboleth Access Management Federations
  - creating clients capable of consuming services protected using Shibboleth Access Management Federations
  - wanting to understand the potential of, and issues associated with, Shibboleth Access Management Federations

#### 5.4.2 Out of scope

The following issues were explicitly left out of the scope for the IE:

- Metadata describing authentication capabilities of services.
- Modifications of existing OGC service specifications (to accommodate authentication issues).
- Authorization, audit or other security functions.
- GeoRM.
- E-commerce solutions. The IE was focussed on Shibboleth Access Management Federations where it was assumed that legitimate users have pre-defined licence arrangements with Federation Service Providers in place. More sophisticated arrangements layered on top of federations enabling various forms of licence negotiations can be envisaged, but were out of scope for the IE.



- Cross access management federation interoperability.

## 6 Methodology

The IE commenced in September 2010 with the first meeting being held in association with the Toulouse Technical Committee meeting. Subsequently, the IE progressed using telcons, email list and a wiki on the OGC portal site.

In addition to these, the usual IE tools, EDINA provided some one-to-one technical support (which then usually formed material for a FAQ) with the objective of assisting the participants develop their OWS clients in time for the Technology Integration Experiment on the 18<sup>th</sup> Nov 2010.

### 6.1 Component development

To further assist the software producers with modifying their OWS clients EDINA established a publicly available documented open source reference implementation of a desktop client. This client is an implementation of the SAML Enhanced Client or Proxy (ECP) profile using the *OpenJump* software and is available here:

<http://esdin.fgi.fi/wiki/index.php/Esdin:AuthIE:Client>

### 6.2 Technology Integration Experiment

This was the main vehicle for advancing the IE. The original intention had been to have a “plugfest”, but after discussion with OGC staff it was decided that it would more appropriate to have an IE culminating in a Technology Interoperability Experiment (TIE).

In discussion it was decided that this should be a virtual event and broadcast as a webinar. During the event, the OSI participants who had modified their client software demonstrated using simple scripts distributed beforehand (table 1) a simple ESDIN SSO use case (table 2) using services within the ESDIN Federation.

Table 1 Example script used during OSI Technology Interoperability Experiment

SSO, Desktop Client, WMS			EDINA	Cadcorp	Envitia
1	Attempt access protected service	User not previously authenticated			
2	User picks IdP				

3	Authenticates				
4	Demonstrates access to data				
5	Attempts access different protected services within the Federation	Already authenticated			
6	Demonstrates access to data				

Table 2 ESDIN Authentication Use Case

Actors:	Key ESDIN Users of pan-European Geographical Data
Description:	For a wide variety of different reasons, individuals at organizations such as the EEA, JRC or EC need to be able to access secure INSPIRE Annex 1 compliant download services on top of pan-European coverage data at large scales. The data will be accessed via a desktop client. As this initiative is funded through the EuroGeographics led ESDIN project, it is assumed that the service providers are mainly European NMCAs
Trigger:	Various, user has need for harmonized INSPIRE compliant pan-European data
Preconditions:	<ol style="list-style-type: none"> <li>1. Pan-European harmonized INSPIRE Annex 1 compliant large scale data available from cooperating NMCAs via basic WFS</li> <li>2. Bi-lateral arrangements between NMCAs in cases where x-border data requests made</li> <li>3. The users organisation and the ExM WFS service provider are part of the same access management federation. In this case, the ESDIN Federation.</li> <li>4. User has access to a desktop client capable of undergoing the Shibboleth/SAML interactions</li> </ol>
Postconditions:	<ol style="list-style-type: none"> <li>1. User has been authenticated and authorized</li> <li>2. Data has been delivered to the users WFS client application</li> </ol>
Normal Flow:	<ol style="list-style-type: none"> <li>1. Users application issues a GetCapabilities request</li> <li>2. User selects their Identity Provider from a list of IdPs</li> <li>3. Authenticates</li> <li>4. The application issues a GetCapabilities request followed by however many DescribeFeatureType, GetFeature</li> </ol>

	requests and responses as necessary to satisfy users requirements
Alternative Flows:	1. Single Sign On. User has recently successfully authenticated and accessed either this or another federation service and therefore gains immediate access to this service without needing to authenticate again.
Exceptions:	1. User not authorised. Authorisation exception 2. Illegal request leading to a service exception 3. Security exception in case of attack
Includes:	
Priority:	High, being able to securely exchange identity information to make authorisation decisions is a fundamental pre-requisite of a large number of SDI scenarios
Frequency of Use:	High
Business Rules:	
Special Requirements:	
Assumptions:	It is assumed that a trust federation comprising the ESDIN partners and cooperating organisations will have been established and is being maintained. To service x-border requests requires infrastructure capable of recognising the special case and forwarding to the appropriate WFS. Pragmatically, this will require bilateral arrangements between NMCAs and prior generation of edge-matched cross-border data.
Notes and Issues:	<p>A single multi-state Federation is assumed here. Cross-federation interoperability is not assumed but is likely to be desirable under several scenarios, for example:</p> <ul style="list-style-type: none"> <li>• Where a key user, eg, the EEA, operates its own federation-like partnership (European Environment Information and Observation Network (EEIONet)).</li> <li>• Where a member state has established its own national federation for purposes of organising how public authorities within that state make their INSPIRE compliant services available</li> </ul>

## 7 Results

The period between the end of the OGC Technical Committee in Bonn and the TIE was short - just over 7 working weeks. In this period the following organisations (excepting EDINA) listed in Table 3 found time to modify their OWS clients.

Table 3 OSI participants who demonstrated software during the TIE

Type of Client	Organisation Name					
	EDINA (opensource)	Snowflake	Cadcorp	con terra	JRC (opensource)	Envitia
WMS	Browser,  Desktop,  Proxy		Desktop	Proxy	Browser	Desktop
WFS	Desktop	Desktop	Desktop	Proxy		

Note the range of different OWS clients demonstrated:

- Proprietary and open source
- Desktop, browser and proxy (EDINA server-side, con terra client-side)

That the approach works was further demonstrated by using an additional separate test federation established in-house by the BKG (the German National Mapping and Cadastral Agency).

The following conclusions can tentatively be drawn:

- Using Shibboleth to protect OWS is practical
- Not particularly difficult on the server side (effectively it is a straightforward Shibboleth installation).
- Browser based OWS clients are not particularly difficult to modify to be able to undergo the Shibboleth/SAML interactions

- More subtle with desktop based clients, but possible with some effort in a relatively short space of time. Especially with assistance to hand and access to a reference implementation
- Highly likely community support and tooling will be available if decision is taken to operationalise this organisational model for SDI.

The following sections provide more detail from each software producing OSI participant concerning their own experience in creating a Shibboleth enabled client during the IE.

## 7.1 EDINA

On behalf of the ESDIN consortium, EDINA initiated the Shibboleth IE on behalf of the ESDIN consortium based on much prior experience. Much of the relevant information, eg, FAQ, source code, debugging assistance, is available from the following URL under the *Identity Management* heading:

[http://esdin.fgi.fi/wiki/index.php/Main\\_Page#Identity\\_management](http://esdin.fgi.fi/wiki/index.php/Main_Page#Identity_management)

## 7.2 Envitia

Envitia supply world class geospatial technologies to customers in mission critical applications, enabling enhanced decision support through the integration of disparate data sources. We do this through our Envitia GI Web Services offering and our MapLink Pro developer kit. A key focus is on information integration for the provision cross-community situational awareness. To meet business goals the sources Envitia has to integrate are more and more often being delivered by on-line resources protected by proprietary mechanisms, and often have complex access restrictions which need to be taken into account in any solution delivery. In addition there is often a range of architectural approaches used to deploy our software, with solutions being deployed on a range of operating systems and environments and involving both light clients (browser based solutions) and fully deployed applications.

A particular problem is having an adequate source of user identity in order to allow/disallow access, and different sources typically have specific communities responsible for identity management. Having a methodology to deal with this diversity in identity information effectively across a range of delivery solutions and providers is essential for long term information integration which is a key element of our offerings. A solution which requires for example the user to repeatedly log in for each source is highly detrimental to an efficient workflow, and so we are keen to avoid this. It also complicates the access management within the application itself (and also to some degree be undesirable from a security perspective) if the client application had to maintain the various identities/passwords for the user for different sources. Given our keen interest in open standards based solutions, we were drawn to the SAML Standard and to the Shibboleth implementation in particular to support federated identity and solve many of these problems.

Many organisations are looking at providing SAML compliant services, and our belief is that if our client software libraries, among others, support SAML 2.0 this will encourage adoption by service provider organisations. As a specialist technology provider Envitia sees the success of open standards as very important element of exploiting our technology, and this is an additional reason for our interest and support of the Shibboleth Interoperability Experiment. Clearly we cannot have control over resources produced and maintained by third parties; but Shibboleth offers these third parties a way to support single sign-on without significant work on their part and also without modifying their existing service implementation. This approach is much easier to “sell” than one which requires more significant implementation changes.

### **7.2.1 Envitia Experimentation with SAML/ECP Profile**

Envitia had been experimenting with SAML 2.0 (or more specifically the Shibboleth implementation of SAML 2.0) as a means to protect web services produced by Envitia and to support Federated Security Single-Sign-On for other resources when this experiment was identified to us. Prior to the Shibboleth Interoperability Experiment, Envitia had successfully prototyped the necessary parts of SAML (2.0) to protect Envitia GI Web services accessed by a browser based application and by our own client (via the ECP Protocol). This was part of internal on-going research and development.

Whilst supporting SAML 2.0 in a web browser environment is relatively straight forward (as it is handled by the browser, and the JavaScript has little to do), web portals on browsers are only one way that distributed resources can be accessed. For high performance, desktop applications are the normal approach. In these cases the SAML Web Browser SSO profile is not appropriate and alternative mechanisms are required.

Envitia’s MapLink product, which already provides client interfaces to the WMS and WFS service types, was extended to support SAML Enhanced Client or Proxy (ECP) exchanges. We also defined a use case and produced a demonstration application which used the client library in order to demonstrate that federated identity would work. The client application was written in C++ using the beta Maplink Pro V7 SDK running on a Windows environment (MapLink Pro 7.0 is due for release in Q3 2011).

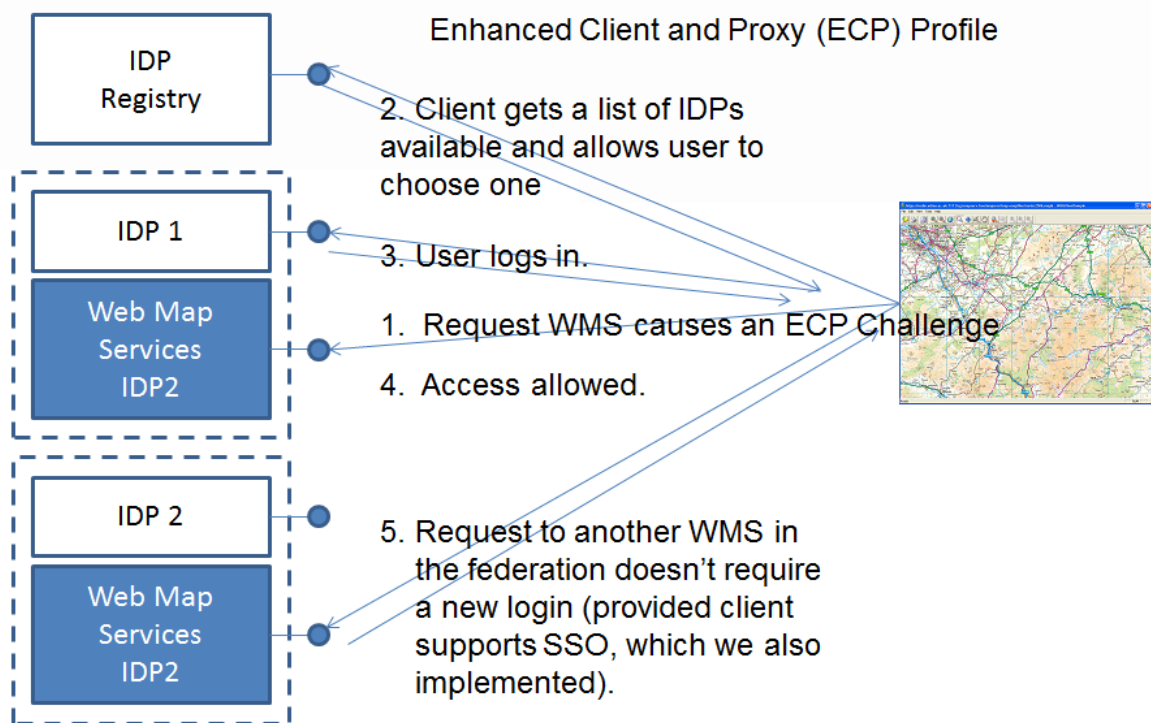
To support understanding of the mechanisms involved the ECP Client application was developed against the same test federation that Envitia used to evaluate the use of SSO in a browser environment. Having full access to both the server and client environments significantly improved support for debugging the client code. It is important to note that no changes were made to the test federation environment (ECP support was included as part of the initial Shibboleth configuration at the SP layer.)

We were, though, interested in the possibility of testing with other federations supporting SAML2 as this is always a better test in a community than simply depending on purely internal implementations/configurations alone. As a result we joined the Shibboleth IE as an ECP Client provider.

### 7.2.2 Engagement in the Shibboleth IE

Envitia took part in the OGC Shibboleth Interoperability Experiment (ShibIE) to subjectively, at least, validate our implementation in the client of mechanisms to manage Federated Security and single sign on. As part of ShibIE, Envitia tested the ECP client described above using the MapLink Pro SDK against the Federated Security and SSO framework set up as part of the experiment. It is important to note that no changes were made to the test federation environment provided under the experiment (ECP support was included as part of the initial Shibboleth configuration at the SP layer).

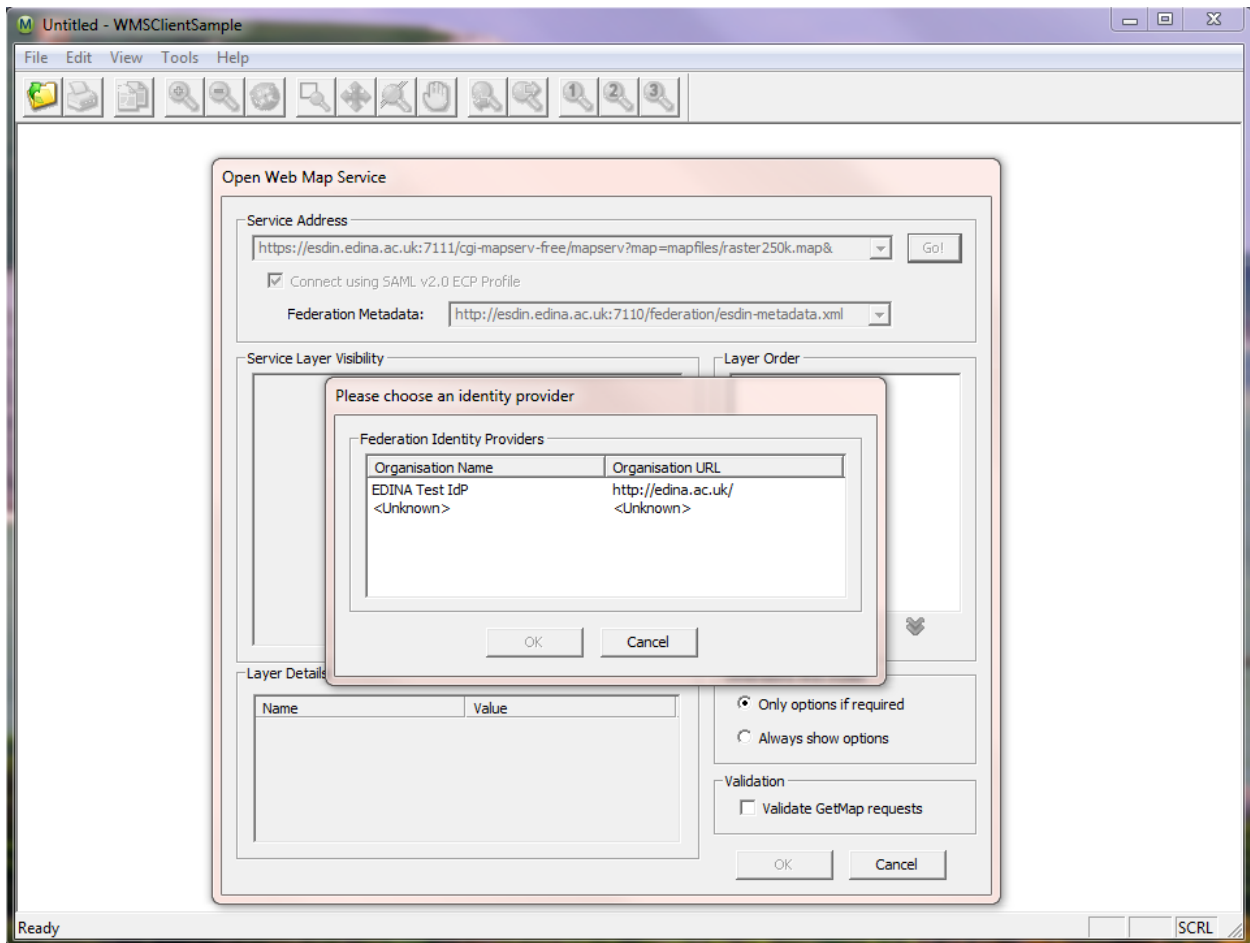
The diagram below shows the general behaviour of the ECP client with the Identity Provider (IDP) and Service Provider (SP)



**Figure 3 - ECP Profile Exchanges**

The test application accessed the WMS resource as normal (in the initial case with a standard WMS GetCapabilities request). Instead of returning the WMS resource as would be expected in an unprotected resource the service provider returned an ECP challenge. The client received the response and identified this as an ECP authentication request. To support the authentication the client application needed to communicate with an appropriate Identity Provider. Available Identity Providers were obtained from the associated federation metadata loaded by the client.

The diagram below shows a screen shot of the client application which identifies the service request, a check box to inform the client that the client would be using the ECP profile, the location of the meta data and a list of the IDPs available in the metadata.

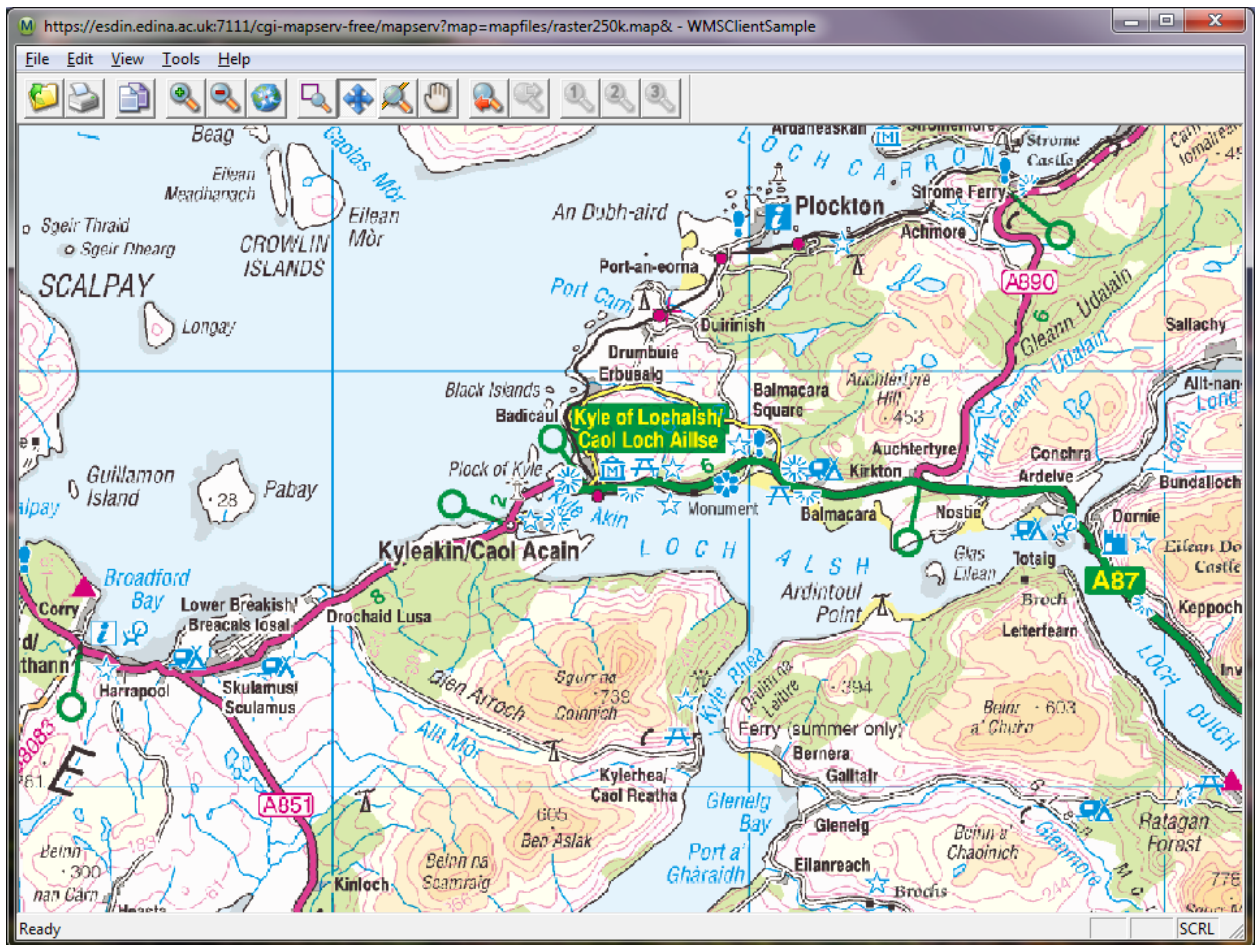


**Figure 4 IDP Selection**

The authentication request received from the SP needed to be modified to remove (and temporarily store) the header information before forwarding the request, together with username and password, to the IDP. The authentication response from the IDP was then edited to re-insert elements from the original authentication request. Specifically these were the RelayState (if present) and its associated attributes (actor, mustunderstand) and the RefToMessageID attribute associated with the Request. Care had to be taken to ensure that merging operation does not invalidate the XML document, this included avoiding additional whitespace and other apparently unimportant formatting information. The modified response was then sent back to the original SP and if the user attributes were appropriate the SP returned the originally requested information.

Future calls to the protected resource were dealt with using cookies managed by the underlying HTTP libraries. The diagram below presents the WMS data as would be expected through an unprotected service.





**Figure 5 WMS Map Display**

The behaviour of how requests to other resources protected by the federation are dealt with is dependent on the client implementation.

### 7.2.3 Envitia Conclusions

The use of the SAML 2.0 ECP profile appears to be a viable mechanism for dealing with federated security over a range of disparate resources. At the client side there were no Shibboleth specific requirements that needed to be incorporated and in principle the solution implemented in the Envitia SDKs for the ECP Client should operate with any SAML2 compliant implementation. The protected resources against which testing was carried out did utilise the Shibboleth components, so it is not possible to say how the client would handle other SAML ECP profile implementations. Comparative testing would need to be carried out on other SAML ECP implementations, however, the expectation is that there should be little or no modification required at the client side to handle other implementations that adhere to the profile.

One issue identified with the testing performed in this trial, was that it was a positive rather than a negative test. The goal was to prove that it did work rather than examine vulnerabilities. This is obviously a target requirement for a future trial.

### **7.3 Joint Research Centre (JRC) - Implementation of Shibboleth-based protected OGC Web Map Services and their access from the INSPIRE GeoPortal**

The Open Geospatial Consortium (OGC<sup>®</sup>) launched on 31<sup>st</sup> August 2010 the Shibboleth Interoperability Experiment (IE) to advance best practice for implementing standards on federated security in transactions involving geospatial data and services.

The aim of the IE was to demonstrate the use of Security Assertion Markup Language (SAML) with OGC Web Services, including use of Shibboleth. The IE was built on best practices from the European Spatial Data Infrastructure Network (ESDIN) project and on results from previous OGC initiatives on authentication. Shibboleth is an open source software package released by the Internet2 Consortium based on the SAML standard from OASIS.

Federated security is relevant for INSPIRE network services therefore it was decided to participate in this IE. In this document we report on the work performed and the knowledge gained through our participation in the shibboleth interoperability experiment.

The JRC contribution focused on a) the implementation of a Shibboleth-based protection system for OGC web mapping services (WMS) and b) accessing protected WMS from the INSPIRE Geoportal. Our experiment was twofold:

1. Server side: installation and configuration of a Shibboleth Service Provider (SP) (to protect a WMS service) and an Identity Provider (IdP) ;
2. Client side: adding support for Shibboleth protected WMS services to the INSPIRE Geoportal Viewer application.

The JRC contribution was wider to what was initially requested by the OGC Shibboleth IE. Having the possibility to work in this field, we took the opportunity to explore additional use cases and perform experiments that were initially out of scope of the Shibboleth experiment.

#### **7.3.1 Use Cases**

To test support for protected services from within the INSPIRE Geoportal Viewer application five use cases were developed.

1. Add protected WMS service “A” (not member of any federation<sup>2</sup>) to Viewer map;
2. Add protected WMS service “B” from federation “Federation1” to Viewer map;
3. Add protected WMS service “C” from federation “Federation1” to Viewer map while service “B” is in use;
4. Add protected WMS service “D” from federation “Federation2” to Viewer map while services “A” and “B” are in use by the Viewer;
5. Add non-protected WMS “E” to the Viewer map while protected services are there.

### Use cases in more detail

1. When accessing a protected WMS “A” from the INSPIRE geoportal viewer, users should be redirected to identity provider (IdP) page/form, specified in the Shibboleth Service Provider (SP) metadata for WMS “A”. After entering username and password for IdP of WMS “A” and the user is authenticated successfully, the WMS layers are added to the geoportal viewer. Follow up requests to WMS “A” from the geoportal viewer do not require further authentication. It is worth noting that this use case does not follow the “IdP initiated SSO” paradigm. It is possible to consider it as part of an “SP initiated SSO” flow (the flow begins with WMS “A” which is a SP). However, as already mentioned, we do not consider WMS “A” inside a federation, so we do not consider this a SSO. It just implements a normal logon procedure. We developed this use case to demonstrate the ability of INSPIRE Geoportal to access a protected WMS, since the original Geoportal implementation (before the experiment) could only access unprotected WMS. Thus, the Geoportal does not play a role as IdP nor SP in this use case.
2. When accessing a protected WMS “B”, users can enter/select a federation resource endpoint, proposed by the geoportal interface – “Federation1”. (Federation for Shibboleth - resource where linkage for number of IdP and SP providers specified). The geoportal viewer shows the page/form for IdP selection based on what is proposed by “Federation1”. After entering username and password for the selected IdP of WMS “B” and successfully authenticated, the WMS layers are added to the geoportal viewer. Follow up requests to WMS “B” from the geoportal viewer do not require further authentication.
3. When accessing protected WMS “C”, users can enter/select federation resource endpoint, as proposed by the geoportal viewer interface – “Federation1”.

---

<sup>2</sup> We consider this is not a federation because the IdP and the SP are from the same organisation (JRC). Technically, it behaves the same as if the IdP and the SP are from different organisations (but those organisations are in the same federation) without the need of the Discovery Service.

Assuming that there is still an active login session running (e.g., the session previously started when WMS “B” has been added to the viewer map), WMS “C” will be added without additional sign-on (SP initiated SSO within a single federation). Here users attempt to access a resource on another SP in the same federation. They already have a current logon session on this federation and they do not need to log on again.

4. When accessing protected WMS “D”, users can enter/select a federation resource endpoint, proposed by geoportal viewer interface – “Federation2”. The geoportal viewer shows the page/form for IdP selection based on what is proposed by “Federation2”. After entering username and password for selected IdP of WMS “D” and authenticated successfully, WMS is added to the geoportal viewer. Follow up requests to WMS “D” from the geoportal do not require additional authentication. We are now in the area of inter-federation interoperability, a use case developed considering potential requirements from the INSPIRE geoportal and was out of scope for the IE. In fact, in the frame of the IE the BKG federation was used merely as an extra way of demonstrating that the client software worked properly with any federation.
5. When accessing an endpoint of a non-protected WMS “E” while a number of protected services have been added to the viewer, users can work with maps of both protected and no-protected WMS services layers till the session for protected services is ended.

### **7.3.2 Testing architecture**

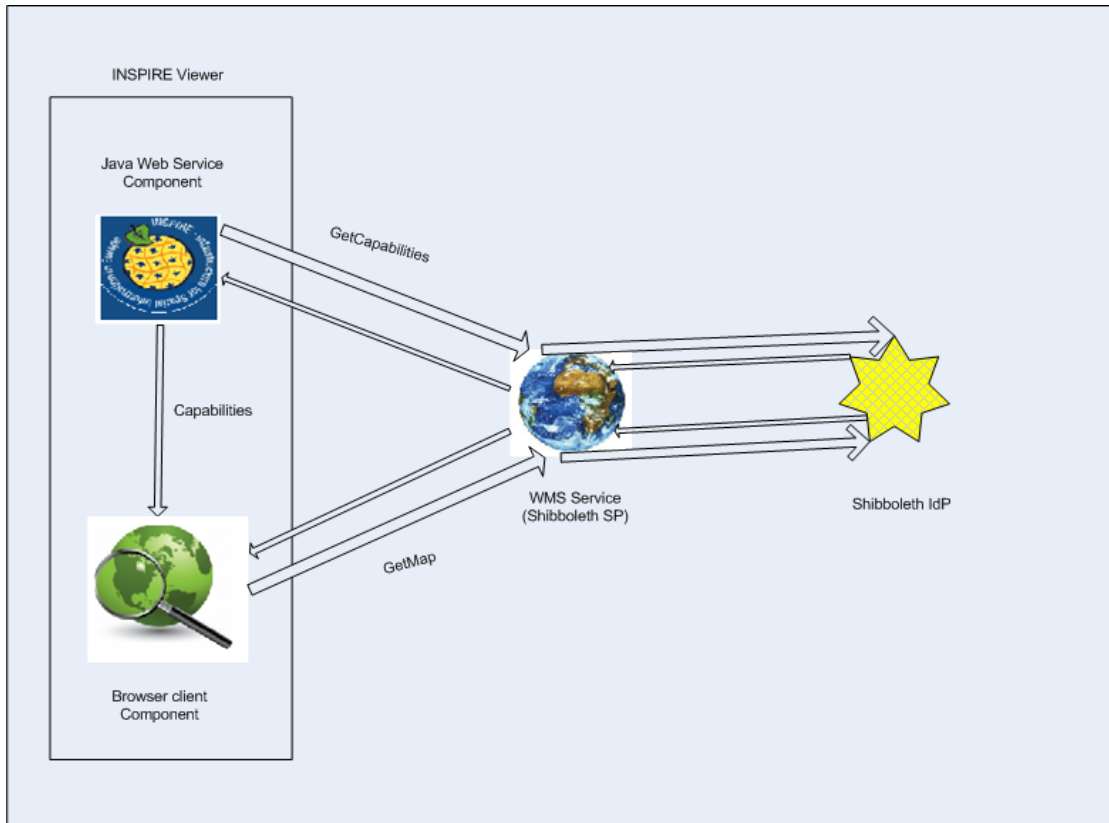
The prototype Geoportal map viewer has two components: a Java Web Service component (a proxy) and a Browser Client component. Shibboleth needs to be supported on both components with different approaches.

#### **Server side**

The Shibboleth Service Provider version 2.3.1 was installed and configured for Windows Server 2008 32-bit with IIS 7.5. A WMS (version 1.3.0) was provided by ArcGIS Server 10. For testing purposes the Shibboleth protected services have been published internally. The Shibboleth IdP and the LDAP server were installed and configured on another Windows Server 2008 32-bit machine. To create a connection between the Java application running on client side and the IdP, the latter needs to support SAML Enhanced Client or Proxy (ECP). We decided to use the Shibboleth ECP extension provided with the software. Shibboleth SP for IIS should be installed with the ISAPI filter option enabled. To make ECP work, SP should be properly configured. SP and IdP have been successfully tested with GetCapabilities and GetMap requests using Web browsers.

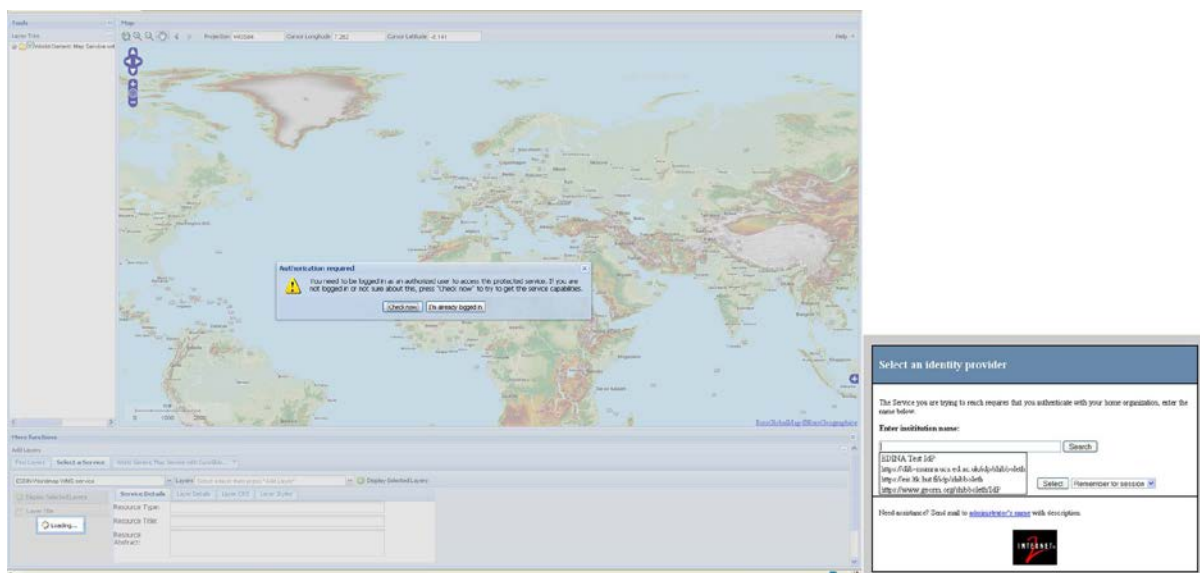
#### **Client side**

The INSPIRE GeoPortal Viewer (a web application developed using JavaScript - OpenLayers and ExtJs- for the client part and Java for the application part) was configured to support WMS protected with Shibboleth. Even though for testing purposes the implementation of Shibboleth protected WMS covered only some aspects, we tested it using the <https://www.georm.org/service/WorldMap?> WMS, together with the EDINA Test IdP and a test account<sup>3</sup>. Figure 7 is a mash-up of a couple of screenshots taken from one of the running tests.



**Figure 6: Enable Shibboleth support for Java Web Service**

<sup>3</sup> From <http://esdin.fgi.fi/wiki/index.php/Esdin:AuthIE:Client>



**Figure 7: INSPIRE GEOPORTAL Viewer client notify user that accessed resource is protected and (on the right) the user is redirected to a defined Federation site, where IdP can be selected**

### 7.3.3 Experienced issues

Implementing the testing architecture we run into some issues. Firstly, with Shibboleth IdP ver. 2.2 and SP ver. 2.3.1 there were some issues on Windows 64-bit machines, so we decided to use Windows Server 2008 32-bit machines for the geoportal Discovery and Shibboleth SP/IdP. Secondly, we experienced also many problems with the so called “same origin policy”<sup>4</sup>. This policy prevents a document or script loaded from one origin from getting or setting properties of a document coming from another origin. The Geoportal domain is certainly different from the Shibboleth SP and IdP domains, so the policy prevents the GeoPortal’s JavaScript code to get information from them. Thus, it is not possible to know if a user is already logged in or not and therefore we can’t provide the login feature in proper time. Some options, tested to overcome this issue are as follows:

1. The login feature or login guide is not provided at all. Let users manage their logged in session themselves.
2. Deploy the service at a Shibboleth aware container and protect the service. At the same time configure the Shibboleth SP to join a Federation (the Shibboleth SP can not join more than one Federation at the same time). In this approach, the session is managed by Shibboleth SP and we don’t need to write any code.

<sup>4</sup> [https://developer.mozilla.org/en/Same\\_origin\\_policy\\_for\\_JavaScript](https://developer.mozilla.org/en/Same_origin_policy_for_JavaScript)

3. The same origin policy can be solved by using the Cross-Origin Resource Sharing (CORS) approach [www.w3.org/TR/cors/](http://www.w3.org/TR/cors/). All SPs should be configured to use CORS. But it only solves partly the Shibboleth issue: when a user tries to access a Shibboleth protected service, the browser needs to be redirected in a complex way which XMLHttpRequest does not support. So we need what is called image hack: raise a request to a document but put it inside an image request. This image request can follow complex redirection and creates cookies in the browser.

Finally, to enable Shibboleth for a Java application, we used the library from Edina<sup>5</sup>. The original Edina library is used for the client side, but the GeoPortal component runs on server side, so it was necessary to adapt it to our structure. We are aware of the fact that it could become a security risk but we needed to remain compatible with the application structure already in place: one on server side and one on client side and both of them need to connect to the WMS. The component on the server side cannot use credentials from the client side because it has to serve many clients at the same time. As the service might serve many clients at the same time, it should be always logged into Shibboleth IdP and the logging process should be transparent to the end-user.

#### 7.3.4 Results and future work

The use cases above were developed and demonstrated during the “plugfest” that took place on the 18<sup>th</sup> of November 2010 as described in section 6. In addition to the Engineering Report, the IE was also presented at the Security WG session during the recent OGC Technical Committee meeting in Bonn and available at [http://portal.opengeospatial.org/files/?artifact\\_id=43044](http://portal.opengeospatial.org/files/?artifact_id=43044).

Moreover, at JRC we will investigate the possibility to extend the architecture we put in place for the aims of this experiment based on the authentication-authorisation-accounting (AAA) technologies employed (if required) by the EU Member States for the Network Services.

## 8 Conclusions

Interoperability Experiments are, by definition, focussed on specific interoperability problems of concern and interest to the OGC membership. This IE was focussed on the use of SAML Access Management Federations as a means of securing OWS across administrative domains so that only properly authenticated principals get access to protected resources. Specifically, it focussed on the use of the open source Shibboleth “reference implementation” of SAML.

Technically, the participants have proven this is feasible and that a range of client software can be modified (with varying degrees of difficulty) to be able to undergo the

---

<sup>5</sup> Available at [http://esdin.fgi.fi/wiki/index.php/Desktop\\_client\\_for\\_protected\\_WMS/WFS\\_Services](http://esdin.fgi.fi/wiki/index.php/Desktop_client_for_protected_WMS/WFS_Services)

Shibboleth/SAML interactions. Some of this client software is available as open source and others proprietary – some of the latter is now available commercially.

Establishing access management federations is however a non-trivial task – there are significant political, legal, organisational and financial implications. If the consensus is that this kind of parallel security infrastructure based on SAML is a necessary concomitant of SDI where protected resources are involved, then the technology is there and demonstrably works; it does not require changes to the OGC specifications and, in the case of Shibboleth, is already in use by a user base numbered in the tens of millions.

Part of the value of maintaining focus and a “separation of concerns” is that it makes problems tractable. There are a large number of related areas of concern and interest to the GI industry, eg, Geo Rights Management, e-commerce, authorisation, electronic licencing, licence negotiation, etc. If SAML access management federations gain widespread acceptance as the preferred means of securely exchanging identity information then it is likely to provide a solid, standards based foundation for making progress in these related areas.